Deutscher Bundestag **Drucksache 19/12269**
19. Wahlperiode 12.08.2019

Kleine Anfrage

der Abgeordneten Uwe Schulz, Joana Cotar und der Fraktion der AfD

Stand der nationalen Risikobewertung der 5G-Netzinfrastruktur

Die vom Bundesministerium für Wirtschaft und Energie (BMWi) am 17. Juni 2019 vorgelegte Ausschussdrucksache 19(23)053 trägt den Titel „Bericht der Bundesregierung zum aktuellen Stand der nationalen Risikobewertung der 5G-Netzinfrastruktur und ggf. erster Schlussfolgerungen daraus auf Grundlage der Empfehlung der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze“.

Nach Ansicht der Fragesteller werden in diesem Bericht allerdings zum aktuellen Stand der nationalen Risikobewertung der 5G-Netzinfrastruktur überhaupt keine Aussagen getroffen, sondern lediglich zum Stand des nach § 109 des Telekommunikationsgesetzes (TKG) aufzustellenden Katalogs von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen und für die Verarbeitung personenbezogener Daten. Der Bericht entspricht damit wortgleich dem bereits mit Ausschussdrucksache 19(23)041 am 12. März 2019 vorlegten „Sachstandsberichts des Bundesministerium für Wirtschaft und Energie zu 5G-Sicherheitsaspekte“, lediglich ergänzt um einige Erläuterungen zu den Empfehlungen der EU-Kommission vom 26. März 2019 zur Cybersicherheit von 5G-Netzen.

In dem aktuellen BMWi-Bericht (Ausschussdrucksache 19(23)053) heißt es wie folgt: „Die von der EU-Kommission bis zum 30. Juni 2019 geforderte nationale Risikobewertung und anschließende Aktualisierung der Sicherheitsmaßnahmen haben wir mit der Veröffentlichung der Eckpunkte für den zukünftigen Katalog an Sicherheitsanforderungen bereits begonnen. Die von der BNetzA am 7. März 2019 veröffentlichten Eckpunkte beinhalten bereits die Kernpunkte der Empfehlung“.

Nach Auffassung der Fragesteller wurden mit diesem Verfahren offenbar Maßnahmen zum Risikomanagement am 7. März 2019 vorgeschlagen, noch bevor die Phase der Risikobewertung am 30. Juni 2019 abgeschlossen wurde.

In dem aktuellen, am 17. Juni 2019 vorgelegten BMWi-Bericht (Ausschussdrucksache 19(23)053), wird ferner mehrfach auf die Frist zum 30. Juni 2019 zur Durchführung der nationalen Risikoanalyse explizit hingewiesen, darunter mit unterstrichener und fettgedruckter Schriftart. Dennoch behauptete eine Vertreterin des BMWi vor dem Bundestagsausschuss Digitale Agenda am 26. Juni 2019, es gäbe diese Frist nicht bzw. sie wäre verschoben. Konkret wurde nur die weitere Frist 15. Juli 2019 genannt, bis zu der der Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) die nationalen Risikobewertungen übermittelt werden sollen.

Eine Methodik zur Analyse und Bewertung von Risiken hat beispielsweise das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe bereits im Jahr 2010 entwickelt und dem Deutschen Bundestag vorlegt (http://dipbt.bundestag.de/dip21/btd/17/041/1704178.pdf). Auf Basis des § 18 des Zivilschutz- und Katastrophenhilfegesetzes (ZSKG) vom 2. April 2009 führt der Bund im Zusammenwirken mit den Ländern seit 2012 jährlich eine bundesweite, ressortübergreifende Risikoanalyse zu unterschiedlichen Szenarien im Bevölkerungsschutz mit Hilfe dieser Methodik durch. Dabei werden Schadensausmaß und Eintrittswahrscheinlichkeit analysiert und das Risiko dementsprechend mit einem Schadenserwartungswert bewertet und in die Kategorien „sehr hoch“, „hoch“, „mittel“, „niedrig“ eingeteilt.

Wir fragen die Bundesregierung:

1. Wann und von wem wurde der Hausleitung des BMWi die laut Empfehlung der EU-Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019H0534&rid=1) gesetzte Frist zum 30. Juni 2019 zur Durchführung der nationalen Risikobewertungen übermittelt?
2. Wann und durch welche Behörden wurde mit der nationalen Risikobewertungen der 5G-Netzinfrastruktur begonnen?
3. Welche Risikofaktoren wurden bei der nationalen Risikobewertung der 5G-Netzinfrastruktur berücksichtigt?
4. Zu welchem Ergebnis hat die nationale Risikobewertung der 5G-Infrastruktur geführt?
5. Welches Verfahren wurde für die nationale Risikobewertung der 5G-Infrastruktur benutzt?
   a) Wurde dieses Verfahren neu entwickelt, und wenn ja, warum wurde nicht auf bereits bewährte Verfahren anderer Bundesbehörden zurückgegriffen?
   b) Entspricht das genutzte Verfahren zur Risikobewertung den Empfehlungen der EU-Kommission vom 26. März 2019 zur Cybersicherheit der 5G-Netze, und falls nein, warum nicht?
6. Sieht die Bundesregierung die Aggregation nationaler Risikobewertungen bei Verwendung nicht EU-konformer und damit uneinheitlicher Verfahren zur Risikobewertung als möglich an, und falls ja, wie?
7. Teilt die Bundesregierung die Auffassung der Fragesteller, dass mit den am 7. März 2019 veröffentlichten Eckpunkten offenbar bereits Maßnahmen zum Risikomanagement vorgeschlagen wurden, noch bevor die Phase der Risikobewertung am 30. Juni 2019 abgeschlossen war, und als wie zielführend bewertet die Bundesregierung diesen zeitlichen Ablauf?
8. Werden die geplanten detaillierten Neuformulierungen im Katalog von Sicherheitsanforderungen vorliegen, bevor die Telekommunikationsunternehmen ihre Verträge mit 5G-Ausrüstern abschließen, und wann wird das sein?
9. Warum wurde der geplante neue Katalog von Sicherheitsanforderungen nicht bereits zum Start der Versteigerung der 5G-Frequenzen vorgelegt, um den Bietern volle Transparenz für ihre Geschäftsmodelle zu ermöglichen?
10. Wann und aus welchen Quellen hat die Bundesregierung erstmals von möglichen Risiken für die deutsche 5G-Infrastruktur durch ausländische Netzwerkausrüster erfahren?

11. Seit wann hat die Bundesregierung Kenntnis von dem Huawei Cyber Security Evaluation Centre (HCSEC), das aufgrund von „ungewöhnlichen Aktivitäten“ der Huawei-Komponenten (core switches) im britischen Telekommunikationsnetzwerk bereits im Jahre 2010 durch die britische Sicherheitsbehörde Government Communications Headquarters (GCHQ) etabliert wurde (www.wired.co.uk/article/huawei-gchq-security-evaluation-uk)?

12. Warum behauptet das BMWi in seinem am 17. Juni 2019 vorgelegten Bericht (Ausschussdrucksache 19(23)053), die Bundesnetzagentur (BNetzA), das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hätten „unverzüglich“ im Zuge der in den vergangenen Wochen geführten Diskussionen um die Netzwerksicherheit gehandelt und die Eckpunkte für den zu überarbeitenden Katalog von Sicherheitsanforderungen abgestimmt, obwohl nach Ansicht der Fragesteller „Diskussionen um die Netzwerksicherheit“ der Bundesregierung schon deutlich länger hätten bekannt sein müssen als nur ein paar Wochen (www.spiegel.de/netzwelt/netzpolitik/5g-in-deutschland-usa-fordern-verzicht-auf-huawei-technik-a-1240977.html)?

    Sieht die Bundesregierung vor diesem Hintergrund eine Bewertung der Abstimmung der Eckpunkte als „unverzügliches“ Handeln als gerechtfertigt an?

13. Wird der Katalog von Sicherheitsanforderungen auch Sanktionen enthalten, und wenn ja, welche?

14. Wie soll nach Ansicht der Bundesregierung mit den dem BSI vorzulegenden „Nachweisen der Vertrauenswürdigkeit“ des Herstellers umgegangen werden, wenn diese Nachweise mit existierenden Vertrauenswürdigkeitsbewertungen deutscher Sicherheitsbehörden kollidieren?

15. Mit welchem technischen, organisatorischen, personellen und finanziellen Mehraufwand bei dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und bei der Bundesnetzagentur (BNetzA) ist durch die Umsetzung der gesteigerten Anforderungen des Katalogs zu rechnen?

16. Ist das BSI und die BNetzA bereits technisch, organisatorisch, personell und finanziell in die Lage versetzt worden, die gesteigerten Anforderungen des Katalogs umzusetzen, und wenn nein, wann wird damit begonnen?

17. Beabsichtigt die Bundesregierung überhaupt, die Produktprüfungen unmittelbar durch das BSI selbst durchführen zu lassen, oder soll das Prüfverfahren, vergleichbar mit dem britischen Modell der Prüfung durch das HCSEC unter Aufsicht des GCHQ, durch das in Bonn ansässige Huawei Security Lab unter Aufsicht des BSI durchgeführt werden?

Berlin, den 18. Juli 2019

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333